Testimony of
Daniel Jaye
Chief Technology Officer
Engage, Inc.

Hearing Before Commerce Committee

United States Senate

June 13, 2000

Thank you, Mr. Chairman. I appreciate the opportunity to testify before you today on these issues of importance to your Committee, to Internet users, and to the future of our Internet economy.

My name is Daniel Jaye. I am the Chief Technology Officer and Co-Founder of Engage, Inc. of Andover, Massachusetts. Engage is a leading provider of technology and services that allow web site operators and advertisers to tailor their commercial and editorial content in innovative ways likely to be of the greatest interest to a visiting Internet user – all without tracking, or ever learning, an individual's identity.

Since co-founding our company in 1995, I have been engaged in the design and development of privacy-sensitive online marketing solutions - including inventing the Internet's first anonymous profiling technology, participating as a founding member of the initial so-called "P3P" specification and as author of the related "TrustLabels" specification (developments I'd like to highlight shortly). I have also actively participated in a number of significant industry online privacy standards initiatives, including the Network Advertising Initiative (NAI). And I have recently served as a member of the Federal Trade Commission (FTC) Advisory Committee on Online Access and Security, and a panelist in the FTC/NTIA Online Profiling Workshop in November 1999.

I would like to address three topics today:

- First, the fundamental role served, and the basic models used, by online network advertisers;

- Second, the technological tools and developments that are bolstering the power of industry – and indeed the power of consumers themselves – to promote privacy- sensitive online practices; and,

- Third, the potent market forces that are compelling online businesses to provide consumers real assurance that they can surf the web without unwittingly sacrificing their personal privacy.

I might note that I offer these comments not in an effort to demonstrate that there could never be a place for legislation in this area, nor out of any concern about the direct impact of proposed privacy

allow advertisers to deliver relevant ads to the right audience. Today, however, three out of four Internet ads remain unsold or undersold. And, not coincidentally, the great majority of web sites remain non-profitable. The traditional advertisers that we must attract to the web will come in requisite numbers only if they can achieve the measurability and effectiveness that they can achieve offline - and something more, as well. Profiling technology enables this advertising and content to be more effectively targeted to consumers' interests, thus offering a vital means for fulfilling the Internet's rich potential – for consumers, advertisers, and web site operators alike.

Different online companies employ different business models and technologies to offer customized news, information and ads on topics of demonstrated specific interest, even when a visitor might be viewing more general interest web pages. And, the types of information collected and used for online profiling can vary among personally identifiable information (PII), non-personally identifiable information (non-PII), or a combination of the two.

- PII is data used to identify, contact, or locate a person, such as name, address, telephone number or e-mail address.
- Non-PII is data that does not identify a particular person and is typically compiled from anonymous clickstream information collected as a browser moves among different web sites (or a single web site).

The collection of online data relies upon the use of "cookies", which are simply small files of information that most web sites place on a user's browser – to provide, in Engage's case, a unique anonymous identifier *or*, importantly, a message that the browser is set to opt-out from collection of any data about its users.

Harnessing Technology To Make Online Advertising Effective *And* Privacy-Sensitive

When I joined with CMGI Chairman & CEO David Wetherell to create Engage in 1995, we were guided by the fundamental proposition that effective, tailored online advertising was vital to the Internet's future – but could ultimately be effective only if consumers found online targeted advertising a valued, customized information service and not an unwelcome intrusion. From the outset, then, we developed an innovative technology to enable online marketers to understand the interests of web site visitors based strictly upon *anonymous*, non-personally identifiable information.

Relying only on the apparent interests, broad demographics, and general location of a visitor reflected in interest profiles, Web site publishers, advertisers, and merchants can customize web pages and offer content, ads, promotions, products and services tailored to the visitor in real-time – and, at the same time, protect the consumer's privacy by not collecting personal (or otherwise sensitive) information of any kind. In fact, in our anonymous model:

- We do not know a consumer's name, address, social security number or any other personally identifiable information;
- We do not maintain information about specific web pages a browser visits or how long a visitor stays;
- We do not collect any sensitive or controversial data, such as personal medical or financial data, ethnic origin, religion, political interest or review of adult content; and,
- We do not merge anonymous profiling data with personally identifiable data, no matter the source.

Instead, our anonymous profiles consist of a score signifying the apparent level of a user's interests in various categories. We simply look to the aggregate amount of time a browser has

spent on different types of content – not who they are, or where in particular they have been on the Web. Our conviction from the start has been that it should never be possible for Engage or anyone else to determine (or even "triangulate") a visitor's real world identity based on our abstracted data.

And we employ additional technological tools and practices to ensure this anonymity. We use firewalls – technological barriers to protect a system – to secure the (already) non-personally identifiable information we collect through a patent-pending technology we call "dual-blind" identification: this way individual web sites we work with do not have access to our interest profiles or know what other sites a user may have visited. There is no user interface through which anyone else can gain access to an individual profile. And, even with these technological protections in place, and only non-personally identifiable data at issue, we also provide consumers effective choice regarding whether to participate. We offer clear information about our data collection practices and an opportunity to opt-out of our anonymous information gathering.

In short, Engage's business model not only accommodates, but is in fact borne of, consumer's interest in protecting their privacy interest.

Privacy-Driven Technological Innovation Is Further Empowering Industry And Consumers Themselves To Raise The Bar

Continued technological innovation promises our online industry – and the web visitors themselves – sophisticated yet simple tools to support consumer privacy interests. I can report first-hand that the online industry has indeed brought to bear in the interest of consumer privacy

the same zeal for technological break-throughs that have characterized – and fueled – the Internet itself. The result: a remarkable progression of emerging solutions that will offer consumers previously unimagined forms of notice, choice and protection of their own personal privacy demands.

Emerging tools offer not only instantaneous and automatic notice and choice, but more than that, they also would empower consumers essentially to set for themselves just what measure of privacy they demand – and to avoid any sites that fail to meet their personal standards. The Platform for Privacy Project (P3P) at the World Wide Web Consortium (W3C) would enable a web server to communicate automatically how it collects and shares user data so users can define what privacy standards they prefer for that particular site or in general. Engage was a co-author of the P3P Protocol Specification.

Beyond this, we are very excited about a specific application of P3P in the context of "TrustLabels" for cookies. To directly respond to the leading concerns over third party data collection and transparency, Engage has authored and is working with other industry leaders on a specification for TrustLabels, which would allow web servers to provide notice to consumers concerned about certain uses of cookies and would allow consumers the ability to accept or reject a site's data practices. This technology critically serves the goal of universal compliance with privacy standards. It permits consumers to compel online businesses to be privacy-sensitive because those businesses that attempt to set a cookie and do not meet consumers' privacy demands will cause a warning alert to be displayed on the computer screen of the user, allowing a choice (probably "NO") to be made solely by the consumer regarding whether to permit the business to collect data. The business will be unable to collect the data it seeks, unless and until it reforms its practices to meet the standards of privacy seal organizations. The bad actor will actually be locked out of the marketplace. This, more

than any regulation, will drive universal compliance with seal programs. And, on the Internet, such technology-based enforcement does not stop at national borders. Certainly this is the sort of technological innovation that no one would wish to discourage with a premature regulatory framework that could stunt this continuing evolution – or, worse yet, a patchwork of such regimes across jurisdictions.

Extending Privacy-Sensitive Practices Through Industry Self-Regulation

Along with this commitment to developing robust technological tools to empower consumers, online industry leaders have relied on a complementary set of additional tools to raise the bar industry-wide for the protection of consumer privacy:

- First, adopting effective standards for industry collection and use of consumer data;
- Second, giving those standards teeth through enforceable and increasingly vigorous seal of approval programs;
- Third, extending the reach of those standards by incorporating them into contracts with other online businesses not already subject to such standards; and,
- Finally but critically, actively educating consumers and business customers about our business and the available means for effectively safeguarding privacy on the Web.

In the few short years over which the Internet has blossomed, the online industry has – through rapidly growing use of these tools – made tremendous strides in voluntary, but self-regulated adoption of "the right way" to do business. And through the Network Advertising Initiative, we are ensuring that our network advertiser segment of the marketplace embraces and expands upon prevailing standards – in a clear, public, and enforceable way.

You will hear in the very near future, I believe, in greater detail about how our NAI standards will effectively incorporate all of the key self-regulatory tools I just described – substantive standards, independent third party certification and enforcement, binding commitments on our customers to follow the same standards, and a campaign to educate the public and our web site customers alike.

The Power of Marketplace Demands For Privacy-Sensitive Practices

I will confess that, for Engage, the standards and practices contemplated by industry largely codify the standards we have set for ourselves from the outset. But by no means does that suggest that this self-regulatory initiative, and the recurring spotlight on our industry's business practices, is not making a difference. To the contrary, as a whole, we are working to set a bar and, in certain respects, raise the commonly prevailing bar. More than that, we are fully unleashing an already significant and growing set of marketplace forces – the force of privacy-sensitivity as a competitive advantage. It is a force that we welcome – indeed one we have long harnessed. It is a force that public policy must take care not to squelch. And it is a force that makes the commitment to self-regulation in our business all the more credible.

Our customers know that consumer comfort and security is critical to use of the Internet. In this competitive climate, those businesses serving consumers online ultimately will embrace only those technologies and practices that can provide tailored and effective online advertising *without* compromising consumer privacy. This is a powerful bottom-line force, as ongoing marketplace developments bear witness.

Conclusion

The potent combination of technological innovation, industry standards, contractual requirements extending those standards, enforceable privacy seal programs, consumer and industry privacy education, and FTC enforcement offers a highly reliable and uniquely effective response to online privacy concerns. These initiatives bolster what are already formidable marketplace checks on online businesses' protection of consumer privacy. The needs of our customers to attract – and not repel – consumers will ensure that we get the job done.

But so too is it critical to ensure that we do not needlessly undermine the *effectiveness* of online advertising by freezing the development of new technological tools to meet consumer and business needs. Instead of setting a floor that turns into a ceiling as well, the power of the market and the dynamism of technological innovation promise continued remarkable developments to protect privacy interests. As I suggested at the outset, the viability of e-commerce, of our advertising-supported Internet, and thus of all the Internet's tremendous economic and societal benefits depends on it.

Thank you.